UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/076,952	02/15/2002	Michael P. Lyle	RECOP020	3408

21912 7590 11/15/2006

VAN PELT, YI & JAMES LLP
10050 N. FOOTHILL BLVD #200
CUPERTINO, CA 95014

EXAMINER	
MERED, HABTE	

ART UNIT	PAPER NUMBER
2616	

DATE MAILED: 11/15/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/076,952	LYLE, MICHAEL P.	
	Examiner	Art Unit	
	Habte Mered	2616	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *8/23/2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *15 February 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The amendment filed on 8/23/2006 has been entered and fully considered.

2. Claims 1-20 are pending.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. **Claims 1-20** are rejected under 35 U.S.C. 103(a) as being unpatentable over Shanklin et al (US 6, 578, 147), hereinafter referred to as Shanklin, in view of Salapura et al (US 6, 904, 040), hereinafter referred to as Salapura.

Shanklin teaches a multi-processor (i.e. parallel processor) intrusion detector with load balancing for high-speed networks.

5. Regarding **claims 1, 14, and 15**, Shanklin teaches a method and system for routing data packets for network flow analysis by a multi-processor system having a plurality of processors **(See Figure 2 and 3; Sensors 21 and 31 in Figures 2 and 3 respectively make up the multi-processor system)**, comprising: receiving a data packet, the data packet comprising data sufficient to identify a network connection with which the data packet is associated **(See Column 4:32-40 and Column 6:9-13)**; and assigning the data to one of the plurality of processors for analysis. **(See Column 3:30, Column 5:22-29, 55-60 and Column 7:54-57)**

Shanklin fails to disclose calculating a hash value based on the data sufficient to identify the network connection with which the data packet is associated and assigning the data based on the hash value to one of the plurality of processors for analysis by using a number of bits of the hash value, wherein the number of bits used is determined at least in part by the number of processors included in the plurality of processors.

Salapura teaches a packet-preprocessing interface for multiprocessor network handler.

Salapura discloses disclose calculating a hash value based on the data sufficient to identify the network connection **(Column 4:25-30)** with which the data packet is associated and assigning the data based on the hash value to one of the plurality of processors for analysis by using a number of bits of the hash value, wherein the number of bits used is determined at least in part by the number of processors included in the plurality of processors. **(See Columns 5:42-45, 6:18-21, 7:2-5)**

It would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Shanklin's system to incorporate hash value calculation based on data sufficient to identify the network connection and using the hash value to identify and assign a processor to a specific session where data belonging to the specific session are routed to the same processor. The motivation being hash value calculation simplifies address lookup as it is low cost to implement and saves processor time as stated in Salapura in Columns 1:40-60 and 2:1-2,50-53 and further distributing the workload among the processors on a per session basis allows it to outperform

conventional network handlers in terms of cost and processing efficiency as stated in Salapura in Column 7:5-10.

6. Regarding **claim 2**, Shanklin discloses a method wherein the data in the data packet is sufficient to identify the network connection with which the data packet is associated comprises address data. **(See Column 3, Lines 25-26)**

7. Regarding **claim 3**, Shanklin discloses wherein the data sufficient to identify the network connection with which the data packet is associated comprises address data associated with a source computer that sent the data packet and address data associated with a destination computer to which the data packet is addressed. **(See Column 3, Lines 25-26, Column 4 Lines 12-15 and 25-30)**

8. Regarding **claim 4**, Shanklin discloses wherein the data packet is sent using the TCP/IP suite of protocols and the data sufficient to identify the network connection with which the data packet is associated comprises an IP address and port number associated with the source computer that sent the data packet and an IP address and port number associated with the destination computer to which the data packet is addressed. **(See Column 3, Lines 25-26, Column 4 Lines 12-15 and 25-30. Shanklin discloses the packets are sent using the TCP/IP protocol and the rest of the limitation is inherent to the protocol)**

9. Regarding **claim 5**, Shanklin teaches all aspects of the claimed invention as set forth in the rejection of claim 1 but fails to disclose a method further comprising storing the data packet in host memory associated with the multi-processor system.

Salapura discloses a method further comprising storing the data packet in host memory associated with the multi-processor system. **(See Figure 2, elements 14 and 25 and Column 4:6-20)**

It would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Shanklin's system to incorporate a method further comprising storing the data packet in host memory associated with the multi-processor system. The motivation to use a host memory shared by all processors is to reduce cost of using different memory with different controllers for different processors and Salapura uses a single DMA controller to interface with the different processors to store and retrieve data from the Direct Memory Access that serves as the host memory as stated in Salapura 4:35-37.

10. Regarding **claim 6**, Shanklin teaches all aspects of the claimed invention as set forth in the rejection of claim 5 but fails to disclose a method, further comprising sending an interrupt message to a driver, the interrupt message comprising data identifying the storage location in host memory in which the data packet is stored.

Salapura discloses a method, further comprising sending an interrupt message to a driver, the interrupt message comprising data identifying the storage location in host memory in which the data packet is stored. **(See Columns 1:32 and 6:22-29)**

It would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Shanklin's system to incorporate a method of sending an interrupt message. The motivation for using an interrupt message is to awaken a

processor for processing data, the end result being savings in processor time and simplification of address lookup as stated in Salapura in Columns 1:32 and 6:22-29.

11. Regarding **claim 7**, Shanklin teaches all aspects of the claimed invention as set forth in the rejection of claim 1 but fails to disclose a method further comprising storing the data packet in host memory associated with the multi-processor system and wherein the step of routing comprises sending to the one of the plurality of processors data identifying the storage location in host memory in which the data packet is stored.

Salapura discloses a method further comprising storing the data packet in host memory associated with the multi-processor system and wherein the step of routing comprises sending to the one of the plurality of processors data identifying the storage location in host memory in which the data packet is stored. **(See Salapura Columns 5;1-10, 6:22-29, and Figure 3, step 60 as well as last step in Figure 4)**

12. Regarding **claim 8**, Shanklin teaches all aspects of the claimed invention as set forth in the rejection of claim 7 but fails to disclose a method wherein the step of sending to the one of the plurality of processors data identifying the storage location in host system memory in which the data packet is stored comprises storing the data identifying the storage location in a work queue associated with the processor.

Salapura discloses a method wherein the step of sending to the one of the plurality of processors data identifying the storage location in host system memory in which the data packet is stored comprises storing the data identifying the storage location in a work queue associated with the processor. **(See Column 6:22-29 and Figure 2, element 15)**

13. Regarding **claim 9**, Shanklin teaches all aspects of the claimed invention as set forth in the rejection of claim 8 but fails to disclose a method wherein the work queue is a circular queue.

Salapura discloses a method wherein the work queue is a circular queue. **(See Column 4:10)**

14. With respect to **claims 7-9**, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Shanklin's system to incorporate hash value calculation based network connection data and storing the data packet in host memory associated with the multi-processor system and the step of routing comprises sending to the one of the plurality of processors data identifying the storage location in a work queue in a host memory in which the data packet is stored. The motivation being these steps simplify address lookup, reduce processor time and provides a more efficient packet handling method in that it keeps packets sequences belonging to the same session intact by assigning the packets to a specific work queue belonging to a specific processor as stated in Salapura in Columns 1:45-61 and 2:50-67

15. Regarding **claim 10**, Shanklin discloses a method further comprising associating the data packet with one or more other data packets associated with the same network connection with which the received data packet is associated to recreate a network flow associated with the network connection. **(See Column 3: 43-46)**

16. Regarding **claim 11**, Shanklin discloses a method further comprising analyzing the network flow to determine if any security-related event has occurred. **(See Column 3, Lines 55-65 and Column 5, Lines 30-40)**

17. Regarding **claim 12**, Shanklin discloses a method, wherein a security-related event is determined to have occurred if the network flow matches a pattern associated with a known attack. **(See Column 5:30-40, Column 6:4-8, and Column 7:60-65)**

19. Regarding **claim 13**, Shanklin discloses a method wherein a security-related event is determined to have occurred if the network flow deviates from normal and permissible behavior under the network protocol under which the data packet was sent. **(See Column 5:30-40, Column 6:4-8, and Column 7:60-65)**

20. Regarding **claims 16 and 17**, Shanklin discloses a system wherein the data sufficient to identify the network connection with which the data packet is associated comprises address data associated with a source computer that sent the data packet and address data associated with a destination computer to which the data packet is addressed. **(See Columns 3:23-25, 4:32-40, 6:9-13, and 7:20-27)**

21. Regarding **claim 18**, Shanklin discloses a system, wherein the data packet is sent using the TCP/IP suite of protocols and the data sufficient to identify the network connection with which the data packet is associated comprises an IP address and port number associated with the source computer that sent the data packet and an IP address and port number associated with the destination computer to which the data packet is addressed. **(In Column 4:12-32 Shanklin discloses that his system uses the TCP/IP suite of protocols including TCP, UDP, IP and ICMP. Examiner takes Official Notice that the TCP and UDP protocols provide port number associated with the source and the destination while IP protocol provides the IP address of**

the source as well as the destination. Please refer to Newton's Telecom dictionary 16th edition on pages 838-839)

22: Regarding **claim 19,** Shanklin discloses a system, wherein the driver is further configured to associate the data packet with one or more other data packets associated with the same network connection with which the received data packet is associated to recreate a network flow associated with network connection. **(See Column 7:54-59)**

23. Regarding **claim 20**, Shanklin discloses a system, wherein the driver is further configured to analyze the network flow to determine if any security-related event has occurred. **(See Column 6:47-56)**

Response to Arguments

24. Applicant's arguments with respect to independent claims 1, 14, and 15 have been considered but are moot in view of the new ground(s) of rejection.

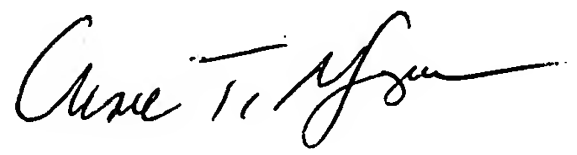
Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Habte Mered whose telephone number is 571 272 6046. The examiner can normally be reached on Monday to Friday 9:30AM to 5:00PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Hassan Kizou can be reached on 571 272 3088. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

HM
11-09-2006



CHAU NGUYEN
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2600